



DEPARTMENT OF HOMELAND SECURITY

STATE AND LOCAL GOVERNMENT OFFERINGS, PRODUCTS, AND SERVICES

The Department of Homeland Security (DHS) partners with the public and private sectors to strengthen the cybersecurity of the Nation's critical infrastructure by facilitating risk management activities that reduce cyber vulnerabilities and minimize the impact of cyber attacks.

The State, Local, Tribal, and Territorial (SLTT) Engagement Program fosters the relationships that secure our Nation's critical infrastructure. Governors and other appointed and elected SLTT government officials receive cybersecurity risk briefings and information on available resources. Through this program, officials have access to cybersecurity initiatives and partnership opportunities with Federal agencies, as well as State and local associations, that will help protect their citizens online.

PARTNERSHIP OPPORTUNITIES

The **Critical Infrastructure Partnership Advisory Council** is a partnership between government and critical infrastructure owners and operators that provides a forum to share information and engage in a broad spectrum of critical infrastructure security and resilience activities, such as the Cross-Sector Cyber Security Working Group. To learn more, email cipac@dhs.gov or visit <http://www.dhs.gov/critical-infrastructure-partnership-advisory-council>.

The **Information Technology Government Coordinating Council** brings together diverse Federal, State, local and tribal government interests to develop collaborative strategies that advance IT critical infrastructure protection. This council serves as a counterpart to the IT Sector Coordinating Council. To learn more, visit <http://www.it-scc.org/>.

The **Critical Infrastructure Cyber Community (C3) Voluntary Program** is the coordination point within the Federal Government for critical infrastructure owners and operators, as well as state, local, tribal, and territorial governments, that are interested in improving their cyber risk management processes. The C3 Voluntary Program assists stakeholders with using the Cybersecurity Framework, and connects them with existing DHS resources for cyber risk management. Learn more at <http://dhs.gov/ccubedvp>.

The **Cybersecurity Partner Local Access Plan** is an initiative that leverages the existing capabilities of State fusion centers as platforms to facilitate classified cybersecurity information sharing to State cybersecurity officials. CPLAP provides States with valuable risk management information on threat context, vulnerability identification and analysis, in addition to information on potential consequences of threats to critical infrastructure Sectors and local governments. For more information, contact the SLTT program at SLTTNCSD@dhs.gov.

The **Multi-State Information Sharing and Analysis Center (MS-ISAC)**, in partnership with DHS and the SLTT Engagement Program, provides cybersecurity support and services to SLTT governments. DHS grant funding to the MS-ISAC provides cybersecurity services for the networks and systems of several States and local governments. For more information, contact the SLTT program at SLTTNCSD@dhs.gov.



The **SLTT Security Clearance Initiative** grants security clearances to State CIOs and CISOs. Clearances received through the initiative will enable SLTT CIOs and CISOs to receive high-value classified and sensitive information about current and recent cyber-attacks and threats, better informing their cybersecurity risk management decisions. For more information, contact the SLTT program at SLTTNCSD@dhs.gov.

CYBER ASSESSMENTS, EVALUATIONS, AND REVIEWS

The **Cyber Security Evaluation Tool (CSET)** provides a systematic and repeatable approach to assess the cybersecurity posture of Industrial Control Systems (ICS) networks. This standalone software tool enables users to assess their network and ICS security practices against industry and government standards and provides prioritized recommendations. To request a CSET CD, email cset@dhs.gov. For all other questions, email cssp@dhs.gov or visit <http://ics-cert.us-cert.gov/Assessments>, where the software is available for download.

The **Cybersecurity Assessment and Risk Management Approach** assists public and private sector partners with assessing, prioritizing, and managing cyber infrastructure risk by providing a picture of sector-wide risks for different categories of cyber critical infrastructure. For more information, email NCSD_CIP-CS@dhs.gov.

SOFTWARE ASSURANCE ASSISTANCE

The **Software Assurance Forum** brings public and private stakeholders together to discuss ways to advance software assurance objectives. Through collaborative events, stakeholders raise expectations for product assurance with requisite levels of integrity and security and promote security methodologies and tools as a normal part of business.

“Build Security In” (BSI) is a collaborative effort to provide tools, guidelines, and other resources, which software developers, architects, and security practitioners can use to build security into software in every phase of development. For information, visit: <https://buildsecurityin.us-cert.gov/swa> or email software.assurance@dhs.gov.

EXERCISES AND TRAINING

The **CyberStorm Exercise Series** focuses on simulated cyber-specific threat scenarios intended to highlight critical infrastructure interdependence and further integrate Federal, State, international, and private sector response and recovery efforts. The series helps participants assess their response and coordination capabilities specific to a cyber incident. Contact CEP@dhs.gov or visit <http://www.dhs.gov/cyber-storm-securing-cyber-space> for more information.

EMERGENCY RESPONSE AND READINESS TEAMS

The **United States Computer Emergency Readiness Team (US-CERT)** operates a 24-7-365 Operations Center, provides situational awareness reports and detection information regarding cyber threats and vulnerabilities, conducts cyber analysis, and provides on-site incident response capabilities to Federal and State agencies. To report suspicious cyber activity, call US-CERT at (888) 828-0870 or email soc@us-cert.gov. The US-CERT's National Cyber Alert System [NCAS] delivers timely and actionable information and threat products, including alerts, bulletins, and tips to users of all technical levels. Visit <http://www.us-cert.gov/cas/signup.html> to subscribe.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) coordinates control systems-related security incidents and information sharing through use of **Fly-Away Teams** with Federal, State, and local agencies and organizations, the intelligence community, the private sector constituents, and international and private sector CERTs. ICS-CERT also operates a **Malware Lab** to analyze vulnerabilities and malware threats to ICS equipment. To report suspicious cyber activity affecting ICS, call the ICS-CERT Watch Floor at (877) 776-7585 or email ics-cert@dhs.gov.

OUTREACH AND AWARENESS

DHS collaborates with its partners, including the National Cyber Security Alliance [NCSA] and the Multi-State Information Sharing and Analysis Center, to support public outreach and awareness activities, including **National Cyber Security Awareness Month** and the Stop.Think.Connect.™ Campaign. The SLTT Engagement Program has been essential to the continued success of this annual event, helping to secure resolutions from all 50 States. The SLTT Engagement Program works to sponsor events and activities throughout the country and disseminate Awareness Month key messages to State and local partners. To learn more or to book a speaker for an upcoming event, visit www.dhs.gov/cyber or www.dhs.gov/stopthinkconnect.

The **National Initiative for Cybersecurity Careers and Studies (NICCS)** works to is an online resource for cybersecurity career, education, and training information. NICCS aims to provide the nation with the tools necessary to ensure citizens and the workforce have more dynamic cybersecurity skills. To learn more about NICCS, visit <http://niccs.us-cert.gov/>.

Government Forum of Incident Response and Security Teams (GFIRST) is a Federal Government information-sharing effort focused on daily information exchange among technical operators across the defense, intelligence, law enforcement, and Federal civilian agency communities. The annual **GFIRST National Conference** gathers partners and analysts to share advances in incident response and best practices to strengthen cybersecurity. For more information, visit: <http://www.us-cert.gov/gfirst>.

Stop.Think.Connect.™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering the American public to be safer and more secure online. The Campaign's main objective is to help you become more aware of growing cyber threats and arm you with the tools to protect yourself, your family, and you community. For more information visit <http://www.dhs.gov/stopthinkconnect>.

